EXHIBIT E

Information Technology Acceptable Use Policy - Global

Background

This Policy is the “Jump Trading Group Information Technology Policy.” It is referred to variously as the “Information Technology Policy,” the “IT Policy,” the “Acceptable Use Policy,” and the “Policy.” Throughout this Policy, the use of “Jump,” “Company,” or the “Firm” refer to all companies within Jump Trading Group. This includes Jump Operations, LLC and every entity under direct or indirect Common Ownership or Control with Jump Operations, LLC at the relevant time.

“Common Ownership or Control” exists with respect to two entities where there is an overlap of at least 50.1 percent of the direct or indirect ownership or control of the equity or voting interests of each entity. Examples of other companies within Jump Trading Group are Jump Trading International Ltd, Jump Trading Europe B.V., JTP Holdings Pte. Ltd, Yue Shen Investment Advisory Services (Shanghai) Co., Ltd., TowerPros LLC, Jump Crypto Holdings LLC (formerly known as 1Hold1 LLC), Jump Capital LLC, and ECW Wireless, LLC.

This Policy governs the access to, authorization to access and use, and acceptable use of the Company’s “Information Technology” systems, including all communications and computer systems owned or operated by the Company. It applies to all Company employees, contractors, subcontractors, consultants, temporary employees, and agency workers and includes all individuals affiliated with third parties who have access to Company Information Technology systems (collectively, “Personnel”).

In addition to the obligations and restrictions imposed directly by this Information Technology Policy, Personnel are also bound by complimentary obligations contained the confidentiality, non-solicitation, and/or non-competition agreements they have signed for the direct or indirect benefit of Jump.

Personnel who are unsure whether something they propose to do might breach Company policy should seek pre-clearance from his/her supervisor or the Legal Department

Violations of the Company's Information Technology Policy alone or in conjunction with the violation of any other policy, agreement, law, or regulation may result in disciplinary action, up to and including immediate termination of employment or other engagement, the institution of civil proceeding, and referral to governmental authorities for potential criminal prosecution.

Key Points:

- Keep Jump data on Jump machines. Do not send or upload Jump data, project documents, or any other sensitive data to your personal email address or a non-approved storage system or otherwise remove it from the Jump systems. This mean, for example, that you can not use any non-Jump provided cloud application (for example for note taking, 'pastebin', document collaboration). Jump provided IT systems for Jump data include Microsoft OneDrive and OneNote, Confluence and internal network shared drives and Jump managed servers/laptops/desktops.
- Note that on mobile devices (including iPads), there is a "work sandbox" that is considered Jump, and the rest of the device (even if Jump owned) is considered personal - this protects both Jump and your personal privacy. Applications must be approved by Jump and installed inside the sandbox to be used for Jump data. This can be confusing as the same named application may exist outside the sandbox: for example, the 'OneNote' application inside the sandbox is approved to use for Jump data (e.g. note taking), but any note taking app outside the sandbox including OneNote signed into a non-Jump account would be out of the sandbox and not permitted. As a general rule, if copy and paste works between the stock phone browser and an application, it is NOT inside the Jump sandbox and must not be used to store Jump data.
- Seek advice if you are not sure: just because a IT system is not physically blocked does not mean its permitted to use it.
- Access to and use of Jump Trading Group’s information technology (“IT”) systems is provided for the sole purpose of performing work for the benefit of Jump Trading Group (“Jump”). Any use of Jump’s IT systems in a manner or for a purpose that is contrary to the best interests of Jump is strictly forbidden. Forbidden uses include, without limitation, using Jump’s IT systems for the benefit of a competitor or of a recruiting firm, to solicit or help others solicit Jump employees, to prepare to compete with Jump, or to engage in any malicious or unlawful act.
- Follow Jump security advice. Do **not** disclose or reuse your passwords. Use 1password, set strong unique passwords when required to, and patch your devices quickly.

- Only access Jump-related systems (including databases and documentation stores) that you must access to fulfill your Jump job responsibilities and then access them only to fulfill your Jump responsibilities. You should ask your supervisor in advance if you are unsure whether you are allowed to access a particular database.
- Be aware that everything you do on a Jump system may be recorded.
- Never share anything obtained from a Jump system with a third party except when necessary to perform your job. Sharing data with third parties when required should be via approved systems, and extreme care should be taken when handling personal data or sensitive Jump IP. If you are in doubt, consult with the Legal Department regarding proper handling procedures.
- Do not post Jump confidential or sensitive information on social media. Be careful of others connecting with you on platforms such as LinkedIn — there are many imposters who pretend to be Jump employees. So, if you don't know the person, you would be wise to check them out internally before connecting with them on such platforms. Please report any suspected imposters to the Legal Department.
- Immaterial personal use of Jump's IT systems in a manner that is in all other respects in compliance with this Policy (including that such use is not intended to or likely to harm Jump or otherwise be contrary to Jump's interests) and all other written Jump policies and all applicable laws and regulations is permissible. For example, it is permissible for an employee to access or transfer information about a personal social dinner reservation or a personal utility bill.

Expectation of Privacy

Jump entities are subject to direct and/or indirect regulation and other legal obligations in multiple jurisdictions to record, save, and/or monitor many types of work communications. In addition, except where prohibited by law, Jump reserves the right to store and review communications for risk management and other oversight purposes Jump. Accordingly, except where applicable law mandates otherwise, Personnel should have no expectation of privacy when using or accessing any Company Information Technology systems, including Jump email, chat, and voicemail. Any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system may be subject to monitoring at any and all times and by any lawful means. This includes (but is not limited to) the use of a computer, telephone, wire, radio, or electromagnetic, photoelectronic, or photo-optical systems.

Monitoring of the activities of Personnel using Company systems may be conducted by authorized Company employees or outside agents (such as regulators) at any time with or without notice. Any information obtained from monitoring may be used for any lawful purpose including, but not limited to, complying with regulatory obligations and the investigation of potential Personnel misconduct, including violations of Company policy. By virtue of using Company Information Technology, Personnel understand and voluntarily consent to such storing, monitoring, and use.

Personnel are encouraged to carry out personal activities such as personal emails, personal calls or connecting to personal websites (such as banking or insurance) via a personal device rather than via Jump provided computer or laptop. If Jump provides Personnel a mobile phone, it is recommended for Personnel to continue to carry a personal device. If Personnel choose to use a Jump issued mobile device for

personal use, this is not forbidden – mobile devices support a 'sandbox' (that is, an electronic barrier) to keep work and personal applications separate. In general Jump does not monitor or have access to applications outside the work sandbox – but Jump continues to own the physical device and in certain situations may require Personnel to return a Jump owned device, including for inspection in connection with suspected misconduct.

Company Confidential and/or Proprietary Information

Company "Confidential and/or Proprietary Information" means all information in any form that is **not** generally known outside of the Company that pertains to any aspect of the Company's business. By way of example, this includes, but, but is not limited to, software, source code, binaries, documentation, configuration, system build information, network information, other technical information, communications with regulatory authorities, employee lists, trading and business strategies, research methods, businesses, business plans, counterparty information, trading team and department lists and membership, and profit and loss information for the Company or any subdivisions thereof, including the profit and loss information for any trading team.

For purposes hereof, Company Confidential and/or Proprietary Information also includes information entrusted to the Company by any third party where the Company has an obligation to keep such information confidential. As between the Company and its employees, all Company Confidential and/or Proprietary Information is the property of the Company. In addition, the property of the Company includes not just physical documents and other physical items but also all electronic documents (including without limitation emails, instant messages, and spreadsheets) sent through or stored in the Company's computer systems that pertain to the Company's business. For the avoidance of doubt, the Company's computer systems include cloud storage used by the Company that is hosted by third parties. The definitions of Confidential and/or Proprietary Information and what constitutes Company property herein supplement and do not replace or limit any definition of such terms in any agreement to which a Company employee is a party.

All electronic Company Confidential and/or Proprietary Information and all other electronic Company property should be stored only on Company approved devices to safeguard their security. The use of unauthorized cloud, removable, or portable media, including, but not limited to, CD/DVD/Blu-ray, USB media, thumb drives, external hard drives, smartphones, memory cards, tablets, cameras (both for storage and taking photos of Company computers or documents), are **prohibited** without the written permission of the Information Security Department, the Compliance Department, or the Legal Department.

You are **not** permitted to keep any copies of Company property on any home or personal device, system, or account (or any device not managed by the Company) without the written approval of the Information Security Department, the Compliance Department, or the Legal Department.

In the event written approval is provided to share confidential or proprietary information with a non-Jump IT system the employee sharing the information has two critical obligations:

- Working with the legal department, get the third party to review and agree to an explicit agreement that ensures that their IT systems adopt a reasonable level of cybersecurity and they understand that they must not retain Jump IP longer than absolutely necessary
- Then, as information is shared, ensure that the third party only retains the information for as long as strictly necessary.
  For example, if it is required and written approval is provided to share confidential Jump IP with a contractor to place on a custom device for some specific piece of work, the employee sharing the data must ensure the contractor or third party confirms they delete this information from any non-Jump IT system as soon as it is not required and they do not build up a large amount of Jump IP (emails, attachments, or other documents shared) on personal devices or emails/cloud accounts.

Company Technical Property

Company-owned or Company-provided "Technical Property" is (or for purposes here if is deemed to be) property of the Company. Company Technical Property includes, but is not limited to, computers, laptops, tablets, and mobile phones. To maintain Company Technical Property in proper working order, ensure that it runs as smoothly as possible, and to maintain its security, these requirements must be followed concerning the use of Company Technical Property:

- All Company Technical Property must be provided by and managed by the Company Tech Services or Linux Department.
- No action should be taken to prevent IT staff from accessing, managing, or monitoring a device, including the use of a device.

- The mere fact that an employee may have the technical ability to log into or otherwise access multiple machines, databases, or files does **not** mean that they are authorized to do so or that they are authorized to review, copy, or download the information contained therein. Personnel should only access equipment and information for which they are explicitly authorized in order to perform their duties.
- Personnel may not install software or take actions to circumvent, disable, or remove any security software or take any other action for the purposes of obscuring their activity (commonly referred to as “hiding their tracks”) . This includes, but is not limited to, the use of data and log wiping utilities, anti-forensics software, rootkits, or malware. It also includes stopping system services or preventing them from starting.
- Devices such as laptops or computers must be configured by the Company Tech Services or Linux Department. Laptops or desktops not configured by the Tech Services department should never be connected to the Jump office network (either physically, via internal secure wifi or via VPN). Connections can be made from non-Jump devices via Citrix, as discussed below.
- All mobile devices with Jump data on them (phones, tablets, etc.) must adhere to the Mobile Device Security Policy.
- Company Technical Property must be always secured and looked after. These devices can be susceptible to theft and leaving them unattended and unsecured in public is not permitted. Any damage or loss must be immediately reported to the Tech Services and Security teams.
- Personnel may not download or install personal software (screen savers, games, sound files, etc.) on Company Technical Property without proper authorization.

Company Networks and Communication Systems Acceptable Use Policy

“Communication Systems” include, but are not limited to, computers, telephones, internet access, email, instant messaging, texting, voicemail, and mobile devices.

“Company Networks,” include wired and wireless networks provided by the Company, excluding the specific wireless networks provided in offices for personal devices and guests.

Company Networks and Communication Systems are intended to be used to access job-related information and for the performance of job-related functions. Use of Company Networks and Communication Systems for personal use is discouraged.

Users should be aware that when access is accomplished using internet addresses and domain names registered to the Company, they are perceived by others to represent the Company. Users may not use the Company Networks for any purpose that would reflect negatively upon Company or its personnel. Unlawful use of Company Networks is prohibited and may expose the employee and the Company to significant legal or reputational liabilities and may result in substantial disciplinary action including the termination of employment.

Below is additional governance regarding the use of the Communication Systems and Company Networks:

- Incidental and occasional personal use of Company mobile phones, computers, email, text messaging and voice mail systems is permitted, but should not interfere or conflict with business use and is not recommended.
- Personnel are expected to act in a professional manner and always use language that reflects positively on themselves and the Company.
- All communications that are required by law or regulation to be recorded and retained must take place via means that are approved by Jump Information Security and Compliance. Approved records-retaining methods include services such as Slack or Company email. You are reminded that all Jump-related communications (including those via text or instant messaging system) are subject to Company inspection.
- Other texting and instant messaging systems may be used only when mandatory retention requirements do not exist. In addition, the use of any such other texting and instant messaging systems is also subject to (1) the guidance of Jump’s Information Security and Compliance departments, and (2) the exercise of good judgment in terms of what information is shared via insecure texting and messaging systems. Although the Compliance department does not intend to review and pre-approve each individual communication (except where required to do so by law or regulation), you are encouraged to reach out to the department prior to the use of any other texting or instant messaging system for a new business subject or if the there is a potential material change in the subject matter or personnel with whom you are already communicating on such systems such that the continued use of such system(s) may no longer be appropriate.

The following activities are examples of prohibited use of Company's Communication Systems and Company Networks. This list is **not** exhaustive:

Personal Use

- Excessive personal use of Company Communication Systems.
- Participating in external chats or newsgroups for non-business-related reasons.
- Engaging in personal commercial activities, such as offering services or merchandise for sale, operating a business, usurping business opportunities, soliciting money for personal gain, or searching for employment outside of the Company.
- Participating in online gambling unrelated to business initiatives.
- Playing online computer or video games.
- External or non-Company email accounts must not be used for business-related matters absent express consent of Compliance.

Activity that is Unlawful and/or a Breach of Duty to Jump

- The use of Communications Systems for any unlawful purpose.
- Exporting software, technical information, encryption software or technology, in violation of Company IT policies, other agreements with the Company, or export control laws.
- Except where necessary for purposes of Company business, sending Confidential and/or Proprietary Information outside of Jump (such as by forwarding an email, uploading a file to a cloud storage provider, or accessing Company data for purposes of copying it and sending it out of Jump).
- The use of Communications Systems directly or indirectly to solicit (including to aid anyone else to solicit) any Company employee to leave the Company or join any other company or venture.
- The use of Communications Systems directly or indirectly to aid a competitor or potential competitor, including to compete or to prepare to compete with the Company.
- The use of Communications Systems in breach of the employee’s fiduciary or other duties to the Company.
- The use of Communications Systems with the intention to cause harm to the Company.
- Dissemination, distribution, or reproduction of copyrighted materials (including articles and software) in violation of copyright laws.
- Any transmission (whether inbound or outbound), or any other use of Communication Systems that contains sexually-explicit images, messages or cartoons, ethnic slurs, racial epithets, or anything that may be construed as harassment or offensive to others based on actual or perceived race, national origin, sex, sexual orientation, age, disability, religious or political beliefs, marital status or any other protected characteristics at any time or is otherwise disruptive, offensive to others, or harmful to morale.

Other Policy Violations

- Impersonating another person, Company employee, or otherwise.
- Participating or engaging in any security breaching type activity to disable, disrupt, harm, or circumvent access controls of any computer system.

File Sharing Policy

Storing and transmitting the Company’s Confidential and/or Proprietary Information Property should only occur both where the material to be shared is approved by an appropriate Company Department (Information Security, Compliance, Legal) and when using a service specifically approved by the Company for this use. Depending on the sensitivity of the data, it may be necessary to password protect or otherwise encrypt the files, such as, for example, when sharing sensitive personal information in connection with KYC/AML checks.

Vendors and third parties may send files using other services. However, personnel must work with the Information Security Department to make a reasonable effort to use a Company-approved file sharing service whenever possible.

When providing confidential information to any third party, an executed Non-Disclosure or Confidentiality Agreement (NDA) is generally required. This agreement can be obtained from the Legal Department, who also hold a list of all agreements currently in force. Please

consult with the Legal Department in advance of sharing confidential information when in doubt whether an NDA is required or is in place.

Social Media Policy

“Social Media” refers to the use of media for social interaction. Examples of Social Media include, but are not limited to, blogs, internet forums, social networks (such as Facebook or LinkedIn), wikis, podcasts, photographs and video, social bookmarking, rating, tweeting, and virtual worlds.

Individuals using Social Media are accountable for what they write and post. Except where prohibited by law, the Company reserves the right to monitor by any means, publicly available and searchable comments, discussions, and posts about the Company, its personnel, and the industry, including competitors, posted on the internet. The Company reserves the right to request that certain subjects be avoided and that certain posts be removed where they contain Confidential and/or Proprietary Information or are otherwise harmful to the Company.

This policy is intended to minimize risk to the Company and its Personnel. If you are uncertain about whether to post or discuss something on Social Media, please direct questions to your manager or the Human Resources Department. Use common sense and good judgment — your statements could have an impact on your reputation as well as the Company's reputation. Remember that posted or published comments may be public information for a long time and could later be used in ways you never intended.

The following are guidelines for using Social Media and are not intended to be exhaustive:

- Always adhere to Company's Handbook, Policies, Compliance Manuals, and any other documentation that governs personal and professional activity at Company.
- NEVER disclose any confidential, proprietary, or sensitive information regarding Company or any regulatory, legal, or financial matter.
- It is permissible to post your job title and to disclose that you work for Company; however, Trading team members should not post the name of the trading team of which they are or were a member. In addition, you should not imply that you speak for the Company unless you are expressly authorized by the Company to do so.
- Do not disclose any information regarding Company that is not already in the public domain as it exists on Company's public websites, the Company’s public filings, or in Company-approved news articles.
- Photographs or videos of the office should never be taken and posted on any internet site.
- Do not post or make comments that may be considered defamatory, obscene, libelous, threatening, harassing, or embarrassing to the Company, other personnel, counterparties, regulators, customers, vendors, contractors, suppliers, or competitors.
- Be aware that Social Media postings may generate press and media attention. If members of the media, including journalists or bloggers, contact you about the Company or any statements you made about Company, refer them to the Company’s media contact or to the Legal Department.
- Do not use the Company logo unless approved by the Company.

Source Code Policy

"Source Code” is any code developed during the course of employment at the Company.

Source Code Ownership

As a general principle all source code developed by Company personnel is the property of the Company. Exceptions for “personal projects” may apply in certain situations in certain jurisdictions. Personnel are encouraged to seek consult with the Legal Department if they believe these exceptions apply.

Source Code Storage

The Company requires all source code to be stored, maintained, and managed in a Company-supported and approved repository — currently GitHub Enterprise.

Personnel are **not** authorized to set up their own repositories outside of the official repositories managed by the Company.

All source code developed by personnel, including all code that forms part of any application used for trading **must**:

- Be checked into the Company managed repository.
- Comply with all review or testing requirements in applicable Compliance software development policies **before** code is placed in production or before any trades are placed using the compiled code.

Source Code Access

The right to access to source code is limited. Personnel should **not** access source code unless it is required for their role (regardless of whether they have the ability to access it). Personnel are **not** permitted to circumvent any controls to access source code.

Open-Source Software Policy

Personnel must take care when using open-source software. Some open-source licenses are fine to use in Jump software. Others have obligations or other reasons that make them not suitable for use in Jump software. In general, Personnel should contact the Legal Department before using new open-source code. For more information and a list of reviewed open-source projects, see Guidance on Open Source Software Licenses on the Legal Department's Confluence page.

Open-Source Collaboration Policy

The ability to contribute to open-source projects is approved on a case-by-case basis. All contributions will be done through a dedicated server allocated for this purpose. Personnel must receive approval from their supervisor, the Information Security Department, and the Legal Department via the Company internal request system before contributing to an open-source project. A detailed process can be located in the Confluence page Open Source Project Collaboration Policy.

Physical Access to Information Technology

The Company seeks to maintain all Company Information Technology in a physically secure manner. Prior to physically accessing Company Information Technology, all personnel must use a uniquely assigned electronic badge to access all Company locations. This badge is exclusive to the assigned individual and must not be shared with anyone. Proper authorization must be granted to access restricted areas such as computer rooms, datacenters, and storage facilities.

Visitors accessing the offices must present a valid form of identification and check-in with the security desk prior to accessing Company. In addition, all visitors must sign a visitor log when they enter Company suites and agree not to disclose any Confidential Information acquired during their visit to the Company's premises. Visitors should not be granted physical access to Company's Information Technology unless supervised by a Company employee.

Clean Desk Policy

When desks or workspaces are left unattended or unoccupied throughout the day or when they are left at the end of the day, any sensitive or confidential materials should be placed in a secure location, such as a locking file cabinet. Materials of this nature should never be left out unattended on a desk or other publicly accessible location. Sensitive materials that are no longer needed and have no regulatory retention requirements should be disposed of in the secure shredder bins made in available in every Company location. Sensitive materials should not be disposed of in normal garbage or recycling bins.

Password and Account ID Policy

Passwords and IDs are used to prevent unauthorized access to Company Information Technology and protect user accounts from misuse. Passwords should be strong, unique, and stored in the firm's password vault (1Password). Individual IDs and passwords must be kept confidential and not shared.

Group IDs, shared IDs, application IDs, administrative IDs, and any other non-unique IDs are only to be used when absolutely necessary for bzusiness functions and no other option exists. Where possible, personnel are required to log into systems with their individual IDs and passwords and switch user to the necessary non-unique ID.

Except when specifically authorized or following proper process, personnel are not permitted to change privileges, gain additional privileges, or revoke/deny other individual's access.

All individuals accessing Company Information Technology are responsible for taking appropriate steps to select and secure their passwords.

General guidelines for the treatment and selection of passwords below:

- Passwords should be stored on the official Company password repository, located at https://jumptrading.1password.com
- Passwords should not be emailed, sent over instant message, or shared except via 1Password and for an authorized business function. No other password manager should be used.
- Do NOT store or write down passwords and leave them in the open.
- Do NOT use your browser's "remember password" feature for any Company Information Technology access. Use the 1Password browser extension.
- Do NOT reuse passwords for Company Information Technology that you use for personal systems or external internet sites.
- Passwords should be constructed using modern complexity requirements. These are documented on Confluence page "1Password: User Pages" under the section "How to choose a strong password." Alternatively, the 1Password password generator can also be used to automatically create a strong password.

Remote Access Policy

"Remote Access" refers to the access of any Company Information Technology from a non-office device.

Remote Access is limited to authorized Personnel only. Remote Access is only permitted using approved supported Remote Access methods. Configuring any system in any way to circumvent Company's supported Remote Access systems is prohibited.

The Company has various methods by which employees may utilize Remote Access.

Citrix

Citrix is a web-based remote access solution that is designed to be used from any remote Windows or Mac machine, including employee-owned personal machines. Citrix provides a layer of protection between the personal machine and the Company network by leveraging the Citrix receiver to allow a person to use specific published applications to interact with the Company network. Company data is never downloaded to the remote machine.

Access to Citrix is achieved via a web portal and two-factor authentication comprised of a username/password combined with a one-time password or hardware token.

Citrix is the only solution for an employee who wants to use a personal device for both personal use as well as accessing the Company network. Personnel should ensure that the device they are using is their own device, a family device, or otherwise trusted and known device. The device must be up to date on patches and not running any software that may be a security risk. It is not acceptable, for example, to connect from an Internet Café type PC or to leave a Citrix session open on a shared computer.

Individuals who use Citrix agree not to violate the End User Agreement, viewable here.

VPN software (e.g. WireGuard)

VPN software such as WireGuard (which may be supplemented or replaced from time to time) allow a Jump computer direct access to the Company network, giving the user the same access that they would have in any of the Company's offices. Using these solutions, a user can copy Company data to his/her local Jump laptop in order to work offline, satisfying the requirement that Company data may only be stored on Company-owned or Company-approved devices.

Personnel using Company-provided devices via VPN must take no action to disconnect the VPN connection. They must also use the device at least monthly to apply the latest security patches. It is strictly prohibited for the user to make any local network connections, for example direct connections to a local NAS or router or attempt to setup software for sharing keyboards or data with personal devices.

Mobile Device Safety

All Personnel are expected to follow applicable federal, state, and local laws or regulations regarding the use of electronic devices at all times. Personnel whose job responsibilities include driving are expected to refrain from using Mobile Devices while driving and should comply with all applicable laws regarding texting by vehicle drivers. Personnel who commit traffic violations or otherwise cause accidents resulting from the use of Mobile Devices while driving will be solely responsible for all liabilities resulting from such actions.

Lost, Stolen, Hacked, or Damaged Mobile Devices

It is important that all mobile devices are stored securely when not in a Jump office. Personnel are expected to protect Mobile Devices from loss, damage, or theft. Personnel must notify the Tech Services Department immediately if a Mobile Device is lost, stolen, hacked, or damaged.

To secure sensitive data, the required Company management software, which allows for a “remote wipe” of data, must be installed on all Mobile Devices used for work purposes. Wiping Company data may affect other applications or data on an affected Mobile Device. The Company is not responsible for loss or damage of personal applications or data resulting from a “remote wipe” and personnel are advised to keep their personal data backed-up.

Information Security Travel Policy

Occasionally Company equipment and personnel will need to travel to a location that is deemed high risk, where the likelihood of the loss of data and the impact from loss of data are both classified as high.

As of January 2021, high risk locations include:

- Mainland China (including Shanghai)
- Hong Kong
- Taiwan
- India
- Russia

Additional countries that are not commonly visited by Jump employees on Company business may also be considered high risk countries.

During travel to such locations, there is the potential for loss of data and/or equipment resulting in significant impact to the Company. This policy defines employee responsibilities, pertaining to information systems, while traveling to and from an area that is deemed high risk to mitigate and lessen the impact if there is an incident resulting in loss of data.

If you are traveling to a country subject to a Department of State Travel Warning (Travel Advisories), contact Tech Services or Information Security, for the country specific appropriate security measures.

Assumptions When Traveling

No device can be protected against all forms of system and information compromise, especially when employees travel to countries that are deemed high risk. Therefore, it must be recognized that the possibility that any device taken to a high-risk country can be compromised in some, potentially undetectable way. The only truly secure option is to refrain from using digital devices when traveling.

Information of particular interest to someone intent on compromising your devices not only includes business data but also the traveler’s ID and password that could be used to directly access Company systems and information resources. When a device is compromised, the attacker may install software on the device that could compromise other systems and data on the Company network when the traveler reconnects his or her device to our network upon return, unless measures are taken to completely restore the device to its original state before it is connected to the Company network.

Travelling Expectations & Jump Advice

The Company forbids Personnel from using a Company laptop containing Company data while residing in a high-risk country. To achieve this, Company offices and travelers should use Citrix. The Company provides loaner devices to travelers, on which they can run Citrix.

Loaner devices may be requested from Tech Services. Regular travelers or individuals based in a high-risk countries can ask Tech Services to issue one of these devices on a long-term basis.

For employees spending more than a few weeks in a high-risk country, using a loaner device is a mandatory requirement, and no exceptions are permitted. If you are relocating to a high-risk country, please return your Jump laptop into Tech Services before leaving. For employees briefly transiting a high-risk country on travel, if there are business reasons to require a Jump laptop, an exception can be granted with the permission of both your supervisor and the head of Tech Services.

In most countries there is no expectation of privacy in internet cafes, hotels, offices, or public places. Hotel business centers and phone networks may be monitored. In some countries, hotel rooms can be searched. If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you are not, you should assume the device has been compromised and report the incident to Information Security.

Best Practices while Travelling

- Before you go, if you are taking any devices with data on them, remove that data from your device. For example, uninstall your Gmail app on a personal phone.
- Shutdown (power off, not “sleep”) any phone or laptop before crossing a border. It is significantly harder for somebody without your PIN and with physical access (e.g. a border agent) to access data on your device when powered off.
- Turn your device’s Bluetooth and Wifi off when not in use.
- Limit the use of public WiFi. If you need to use public WiFi, avoid providing credentials to sites that require username and passwords, as this information may be intercepted.
- Do not use thumb drives given to you — they may be compromised. Do not use your own thumb drive in a foreign computer for the same reason. If you’re required to do it anyway, please notify Information Security as soon as possible.
- Do not leave your electronic devices unattended.
- Be aware of who is looking at your screens, especially in public.
- Do not plug your device via USB into a public kiosk or charging stations as there might be a hostile computer on the other end.
- If your device or information is lost or stolen, report it immediately to Tech Services and Information Security. This should be reported even if the device is later recovered.

Reporting Violations

The Company requests and strongly urges employees to report any violations or perceived violations of the Information Technology Policy to managers, the Human Resources Department, the Information Security Department or the Legal Department. The Company will investigate and respond to all reported violations of any Company policy.

Information Security Training Policy

In accordance with various governmental regulations and NIST Cybersecurity Framework guidelines, information security awareness training shall be conducted on a regular basis. This training will include:

- **First day** — New Hire Orientation
- **Within 2 months of starting** — JumpStart training, which includes security awareness training
- **Quarterly** — Anti-Phishing training (typically a simulated phishing attack)
- **Annual** — Company-wide cybersecurity awareness training combined with annual compliance training

Training will include topics such as:

- Recognizing risks such as phishing emails and malware
- Password Protection
- Software/Hardware Vulnerabilities
- Mobile and Physical Security